Liikenne- ja viestintäministeriö E-KIRJELMÄ LVM2006-00203

VLY Miettinen Kirsi 19.06.2006
Korjattu versio: jakelukorjaus

EDUSKUNTA
Suuri valiokunta

Viite
Komission asiakirja KOM(2006) 251 lopullinen
Asia
Komission tiedonanto neuvostolle, Euroopan parlamentille, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle:
Turvallisen tietoyhteiskunnan strategia – ”Lisää vuoropuhelua, yhteistyötä ja vaikutusmahdollisuuksia”

U/E-tunnus: **EUTORI-numero:**

Ohessa lähetetään perustuslain 97§:n mukaisesti selvitys eduskunnan suurelle valiokunnalle asiakohdassa mainitusta Euroopan komission tiedonannosta sekä tiedonannon suomen- ja ruotsinkielinen versio.

Vt. apulaisosastopäällikkö,
Viestintäneuvos Kristiina Pietikäinen

LIITTEET Viitekohdassa mainitun komission asiakirjan suomen- ja ruotsinkielinen versio sekä tiedonantoa koskeva perusmuistio

Asiasanat	sähköinen viestintä, tietosuoja
Hoitaa	**LVM, OM, VM**
Tiedoksi	EUE, KTM, MMM, OPM, PLM, SM, STM, TH, TM, UM, VNEUS

Liikenne- ja viestintäministeriö PERUSMUISTIO LVM2006-00202

VLY Miettinen Kirsi 19.06.2006
EI JULKINEN

Asia
Komission tiedonanto neuvostolle, Euroopan parlamentille, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle:
Turvallisen tietoyhteiskunnan strategia – ”Lisää vuoropuhelua, yhteistyötä ja vaikutusmahdollisuuksia”

Kokous

Liitteet
KOM(2006) 251 lopullinen

Viite
Komission asiakirja KOM(2006) 251 lopullinen

EUTORI/Eurodoc nro:

-

U-tunnus / E-tunnus:

-

Käsittelyn tarkoitus ja käsittelyvaihe:

Komissio on julkaissut 31.5.2006 tietoturvaa koskevan tiedonannon ”Turvallisen tietoyhteiskunnan strategia – ”Lisää vuoropuhelua, yhteistyötä ja vaikutusmahdollisuuksia”.

Asiakirjat:

Komission tiedonanto neuvostolle, Euroopan parlamentille, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Turvallisen tietoyhteiskunnan strategia – ”Lisää vuoropuhelua, yhteistyötä ja vaikutusmahdollisuuksia” KOM (2006) 251 lopullinen

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely:

-

Käsittelijä(t):

Liikenne- ja viestintäministeriö, neuvotteleva virkamies Kirsi Miettinen,
puh. 160 28570
Liikenne- ja viestintäministeriö, Viestintäneuvosto Juhapekka Ristola
puh. 160 28348

Suomen kanta/ohje:

-

Pääasiallinen sisältö:

Komission yllämainittu tietoturvatiedonanto julkaistiin 31.5.2006. Se on varsin lyhyt (vain noin kymmenen sivua) ja varsin yleisluontoinen. Asiaan liittyy myös tausta-asiakirja SEC(2006)656 (Commission staff working paper), jota ei ainakaan toistaiseksi ole saatavissa Suomeksi.

Dynaaminen lähestymistapa tietoturvalliseen tietoyhteiskuntaan:
Komissio hahmottaa tiedonannossaan kolme otsikkoa, joiden alle tehtävät toimenpiteet sijoitetaan. Nämä ovat vuoropuhelu, *yhteistyö ja vaikutusmahdollisuuksien lisääminen*. Kokonaisuudessaan lähestymistapana on ”sateenvarjomalli”, johon myös Suomessa on pyritty kansallisen tietoturvastrategian luomisesta lähtien. Komissio on nyt myös havainnut tämän lähestymistavan edut, jolloin muun muassa odotettavissa olevat tiedonannot roskapostista ja tietoverkkorikollisuudesta voidaan hahmottaa myös osana tietoturvaa. Edelleen komissio painottaa sitä, että kaikkien toimijoiden mukana olo on ensiarvoisen tärkeää: teollisuuden, kansallisten hallitusten, komission, ENISAn, sekä kansainvälisten toimijoiden (eritt. WSIS).

Vuoropuheluun kuuluvat kansallisten verkko- ja tietoturvaan liittyvien poliitikkojen vertaileva arviointi sekä rakenteellinen monenvälinen sidosryhmien keskustelu. *Yhteistyön* osalta komissio ilmoittaa pyytävänsä ENISAA luomaan luottamuksellisen kumppanuussuhteen jäsenvaltioihin ja sidosryhmiin tavoitteena asianmukainen tietojenkeruujärjestelmä sekä pyytävänsä jäsenvaltioita, yksityistä sektoria ja tutkimusyhteisöä luomaan strategisen kumppanuuden. Lisäksi ENISAn olisi tutkittava, onko mahdollista toteuttaa eurooppalainen tiedonjako- ja hälytysjärjestelmä.

Vaikutusmahdollisuuksien lisäämisen osalta jäsenvaltioiden tulisi osallistua aiemmin mainittuun vertailevaan arviointiin, edistää tiedotuskampanjoita, käynnistää sähköisiä hallintopalveluja ja edistää hyviä tietoturvakäytäntöjä sekä kannustaa verkko- ja tietoturvaohjelmien kehittämistä osana korkea-asteen koulutusta. Yksityisen sektorin puolestaan tulisi tehdä aloitteita, jotta voitaisiin kehittää asianmukainen määritelmä ohjelmistotuottajien ja internet-palvelun tarjoajien vastuusta, edistää monimuotoisuutta, avoimuutta, etc. sekä lisätä tietoturvaa tehostavien tuotteiden & palveluiden käyttöä, levittää hyviä tietoturvatoimintoja, edistää liikealan koulutusohjelmia, pyrkiä luomaan kohtuuhintaiset turvavarmentamisjärjestelmät sekä ottaa vakuutusala mukaan kehittämään asianmukaiset riskienhallintavälineet.

Päätelmät:
Tiedonannossa on myös päätelmä–osio, mutta sen sisältö on erittäin niukka. Siinä korostetaan uudelleen sidosryhmien monenvälistä lähestymistapaa. Lisäksi komissio lupaa neuvostolle ja parlamentille raportin tehdyistä toimista vuoden 2007 puolivälissä.

Kansallinen käsittely:

-

Eduskuntakäsittely:

-

Käsittely Euroopan parlamentissa:

-

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema:

-

Taloudelliset vaikutukset:

-

Muut mahdolliset asiaan vaikuttavat tekijät:

Tietoturva on yksi Suomen puheenjohtajuuskauden prioriteetista sähköisen viestinnän sektorilla. Suomen tarkoituksena on, että teleministerineuvosto hyväksyisi tietoturvasta komission tiedonannon pohjalta neuvoston päätöslauselman joulukuun kokouksessaan.

Asiasanat
Hoitaa

Tiedoksi

EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel, 31.5.2006
KOM(2006) 251 lopullinen

KOMISSION TIEDONANTO NEUVOSTOLLE, EUROOPAN PARLAMENTILLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE

Turvallisen tietoyhteiskunnan strategia – "Lisää vuoropuhelua, yhteistyötä ja vaikutusmahdollisuuksia"

{SEC(2006) 656}

SISÄLLYSLUETTELO

KOMISSION TIEDONANTO NEUVOSTOLLE, EUROOPAN PARLAMENTILLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE

Turvallisen tietoyhteiskunnan strategia – "Lisää vuoropuhelua, yhteistyötä ja vaikutusvaltaa"

1. JOHDANTO

Tiedonannossa "i2010 – kasvua ja työllisyyttä edistävä eurooppalainen tietoyhteiskunta"[1] korostettiin, kuinka tärkeää verkko- ja tietoturva on yhtenäisen eurooppalaisen tietoalueen perustamisen kannalta. Verkko- ja tietojärjestelmien käytettävyys, luotettavuus ja turvallisuus ovat yhä keskeisemmässä asemassa talouksiemme ja yhteiskunnan rakenteiden kannalta.

Tämän tiedonannon tarkoituksena on antaa uutta vauhtia vuonna 2001 tiedonannossa "Verkko- ja tietoturva: Ehdotus eurooppalaiseksi lähestymistavaksi"[2] esitellylle Euroopan yhteisön strategialle. Tässä tiedonannossa tarkastellaan tietoyhteiskunnan turvallisuusuhkien nykytilaa ja määritellään, mitä lisätoimenpiteitä verkko- ja tietoturvan parantamiseksi olisi toteutettava.

Kunnianhimoinen tavoite on jäsenvaltioiden ja Euroopan yhteisön tasolla saadun kokemuksen perusteella kehittää edelleen Euroopalle dynaamista ja kokonaisvaltaista turvallisuuskulttuuriin pohjautuvaa strategiaa, joka perustuu **vuoropuheluun, yhteistyöhön ja vaikutusmahdollisuuksien lisäämiseen.**

Euroopan yhteisö on kehittänyt kolmitahoisen lähestymistavan tietoyhteiskunnan turvallisuushaasteiden käsittelemiseksi: erityiset verkko- ja tietoturvatoimenpiteet, sähköisen viestinnän sääntelyjärjestelmä (joka sisältää myös yksityiseen ja tietosuojaan liittyvät kysymykset) ja tietoverkkorikollisuuden torjunta. Vaikka näitä kolmea näkökohtaa voidaan tietyssä määrin kehitellä erikseen, ne ovat siinä määrin toisistaan riippuvaisia, että tarvitaan koordinoitua strategiaa. Tässä tiedonannossa esitetään tuo strategia, ja luodaan siten puitteet verkko- ja tietoturvaa koskevan yhtenäisen lähestymistavan viemiseksi eteenpäin ja viimeistelemiseksi.

Vuoden 2001 tiedonannossa verkko- ja tietoturva määritellään *verkon tai tietojärjestelmän tietyn tasoiseksi kyvyksi kestää onnettomuuksia tai ilkivaltaa, jotka vaarantavat tallennettujen tai siirrettyjen tietojen ja muiden verkoissa ja tietojärjestelmissä tarjottujen tai välitettävien palvelujen käytettävyyden, aitouden, eheyden ja luottamuksellisuuden.* Euroopan yhteisö on viime vuosina toteuttanut joukon toimia parantaakseen verkko- ja tietoturvaa.

Sähköisen viestinnän sääntelyjärjestelmään, jonka tarkistus on parhaillaan käynnissä, sisältyy turvallisuuteen liittyviä säännöksiä. Erityisesti henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annettu direktiivi[3] velvoittaa yleisesti saatavilla olevien

---

1 KOM(2005) 229 lopullinen, 1.6.2005.
2 KOM(2001) 298 lopullinen, 6.6.2001.
3 Direktiivi 2002/58/EY.

sähköisten viestintäpalvelujen tarjoajan varmistamaan tarjoamiensa palvelujen turvallisuuden. Säännöksiä roskapostin[4] ja vakoiluohjelmien[5] torjumiseksi on annettu.

Luottamus ja turvallisuus ovat tärkeitä myös Euroopan yhteisön tutkimus- ja kehitysohjelmissa. Kuudennessa tutkimuksen puiteohjelmassa näitä kysymyksiä käsitellään useissa hankkeissa. Turvallisuusaiheista tutkimusta vahvistetaan edelleen seitsemännessä puiteohjelmassa perustamalla Euroopan turvallisuustutkimusohjelma (ESRP)[6]. Lisäksi Safer Internet plus -ohjelma tukee verkostointihankkeita ja parhaiden toimintatapojen vaihtoa tietoverkkojen haitallisten sisältöjen torjumiseksi.

Turvallisuusuhkiin vastaamiseksi Euroopan yhteisö muun muassa päätti vuonna 2004 perustaa Euroopan verkko- ja tietoturvaviraston. Virasto osallistuu sellaisen verkko- ja tietoturvakulttuurin kehittämiseen, josta on hyötyä Euroopan unionin (EU) kansalaisille, kuluttajille, yrityksille ja julkisen sektorin organisaatioille.

EU:lla toimii aktiivisesti myös näitä aiheita käsittelevillä kansainvälisillä foorumeilla, kuten OECD:ssä, Euroopan neuvostossa tai YK:ssa. Tietoyhteiskuntahuippukokouksessa Tunisissa EU tuki voimakkaasti keskusteluja verkkojen ja tietojen käytettävyydestä, luotettavuudesta ja turvallisuudesta. Tunisin toimintaohjelma[7] ja Tunisin sitoumus sisältävät maailmanlaajuista tietoyhteiskuntaa koskevan poliittisen keskustelun seuraavat vaiheet, jotka maailmanjohtajat hyväksyivät. Toimintaohjelmassa korostetaan tarvetta jatkaa tietoverkkorikollisuuden ja roskapostin torjuntaa, samalla kun varmistetaan yksityisyyden suoja ja sananvapaus. Siinä todetaan tarve saavuttaa yhteinen käsitys Internetin turvallisuuskysymyksistä ja lisätä yhteistyötä, jotta helpotettaisiin tietoturvaan liittyvän tiedon keräämistä ja levittämistä sekä turvallisuusuhkien torjumiseen tähtäävien hyvien toimintatapojen vaihtoa kaikkien sidosryhmien kesken.

2. TIETOYHTEISKUNNAN TURVALLISUUDEN PARANTAMINEN: KESKEISET HAASTEET

Kansainvälisistä, eurooppalaisista ja kansallisista ponnisteluista huolimatta turvallisuus on edelleen haastava ongelma.

Ensinnäkin tietojärjestelmiin kohdistuvien hyökkäysten motiivina on yhä enemmän hyöty pikemminkin kuin vain halu tuottaa häiriötä sen itsensä vuoksi. Tietoja haravoidaan laittomasti ja yhä enemmän käyttäjän tietämättä, samaan aikaan kun erilaisten haittaohjelmien[8] määrä (ja kehitystahti) kasvaa nopeasti. Roskaposti on tästä kehityksestä hyvä esimerkki: siitä on tullut väline virusten levittämiseen ja petolliseen ja rikolliseen toimintaan, kuten vakoilu-, verkkourkinta-[9] ja muiden haittaohjelmien levittämiseen. Sen laaja

---

4 Ei-toivottua markkinointiviestintää.

5 Vakoiluohjelmat ovat seurantaohjelmia, jotka otetaan käyttöön ilmoittamatta tästä asianmukaisesti käyttäjälle tai pyytämättä tämän hyväksyntää, sekä siten, ettei käyttäjä voi valvoa ohjelmien toimintaa.

6 ESPR:ää valmistellaan turvallisuutta koskevan tutkimuksen valmistelutoimen yhteydessä ajanjaksolla 2004–2006.

7 *Kohti maailmanlaajuista kumppanuutta tietoyhteiskunnan alalla: Tietoyhteiskuntahuippukokouksen (WSIS) Tunisin vaiheen jatkotoimet.* KOM(2006) 181 lopullinen, 27.4.2006.

8 Haittaohjelma on vihamielinen, haitallinen ohjelma.

9 Verkkourkinta (*phishing*) on Internet-petoksen muoto, jolla pyritään varastamaan arvokkaita tietoja, kuten luottokorttien ja pankkitilien numeroita, käyttäjätunnuksia ja salasanoja.

levinneisyys nojaa yhä enemmän botnet-verkkojen[10] käyttöön, toisin sanoen hyökkäyksille alttiita palvelimia ja tietokoneita käytetään välittäjinä niiden omistajien tietämättä.

Kannettavien laitteiden (muun muassa 3G-matkapuhelinten ja kannettavien videopelien) ja matkaviestinverkkopalvelujen käyttö lisääntyy jatkuvasti, mikä asettaa uusia haasteita, kun IP-pohjaiset palvelut kehittyvät nopeasti. Näistä voi mahdollisesti jatkossa kehittyä tavallisempi hyökkäysreitti kuin henkilökohtaisista tietokoneista, koska viimeksi mainittujen turvataso on jo merkittävän korkea. Kaikki uudet viestintä- ja tietojärjestelmät tarjoavatkin väistämättä uusia mahdollisuuksia vihamielisille hyökkäyksille.

Toinen merkittävä kehityssuunta on toimintaympäristöön sulautetun tietotekniikan käyttöönotto. Siinä älykkäät laitteet hyödyntävät läsnä-älyä tietokone- ja verkkotekniikan tuella (esim. RFID[11], IPv6 ja anturiverkot). Täysin yhteenliitetty ja verkotettu arkielämä lupaa merkittäviä mahdollisuuksia, mutta se luo myös uusia turvallisuuteen ja yksityisyydensuojaan liittyviä riskejä. Vaikka yleiset käyttöjärjestelmät ja sovellukset edistävät yhteenliitettävyyttä ja tieto- ja viestintätekniikan käyttöönottoa, ne voivat myös lisätä riskejä. Mitä enemmän esimerkiksi ostetaan kaupasta valmiita ohjelmistoja, sitä suurempia ovat vaikutukset, kun niiden heikkouksia hyödynnetään tai ne eivät toimi. "Monokulttuurien" syntyminen käyttöjärjestelmiin ja ohjelmistoihin voi suuresti helpottaa turvallisuusuhkien, kuten haittaohjelmien ja virusten, lisääntymistä ja leviämistä. **Monimuotoisuus, avoimuus ja yhteentoimivuus ovat turvallisuuden olennaisia tekijöitä, ja niitä olisi edistettävä.**

Tietotekniikka-alan merkitys Euroopan taloudelle ja eurooppalaiselle yhteiskunnalle kokonaisuudessaan on kiistaton. Tietotekniikka on innovaation tärkeä osa, ja se edustaa lähes 40:tä prosenttia tuottavuuden lisäyksestä. Lisäksi tämä erittäin innovatiivinen ala vastaa yli neljännestä Euroopan koko t&k-panostuksesta, ja sillä on keskeinen asema koko taloudessa taloudellisen kasvun ja työpaikkojen luomisessa. Yhä useammat eurooppalaiset elävät todellisessa tietoon perustuvassa yhteiskunnassa, jossa tietotekniikan käyttö on nopeasti lisääntynyt inhimillisen sosiaalisen ja taloudellisen vuorovaikutuksen keskeisenä toimintona. Eurostatin mukaan 89 prosenttia EU:n yrityksistä käytti Internetiä aktiivisesti vuonna 2004, ja noin 50 prosenttia kuluttajista oli äskettäin käyttänyt Internetiä.[12]

Verkko- ja tietoturvaloukkausten vaikutus voi ulottua talousnäkökohtia paljon pitemmälle. Yleisesti pelätään, etteivät käyttäjät turvallisuusongelmien takia halua ottaa käyttöön tietotekniikkaa, kun taas käytettävyys, luotettavuus ja turvallisuus ovat ehdottomia edellytyksiä, jotta perusoikeudet voidaan verkossa taata.

Lisäksi elintärkeät infrastruktuurit (kuten liikenne, energia) ovat yhä riippuvaisempia niiden kunkin tietojärjestelmien eheydestä, koska eri verkot liitetään yhä enenevässä määrin yhteen.

Euroopassa sekä liikeyritykset että kansalaiset aliarvioivat edelleen riskejä. Tämä johtuu monista syistä, joista tärkein näyttää olevan yritysten osalta se, että turvallisuuteen tehtyjen investointien tuottoa on vaikea hahmottaa, ja kansalaisten osalta se, että he eivät ole tietoisia omasta vastuustaan kokonaisvaltaisessa turvallisuusketjussa.

---

10 Botnet-verkot ovat verkkoapulaisten käyttämiä verkkoja. Verkkoapulaiset eli botit (<- engl. *robot*) ovat etäohjattavia sovelluksia, jotka asennetaan uhrikoneelle salaa.

11 *Radio Frequency Identification* (radiotekniikkaan perustuva etätunnistus).

12 Eurostat, *Internet activities in the European Union*, 40/2005.

Kun otetaan huomioon tietotekniikan ja tietojärjestelmien läsnäolo kaikkialla, verkko- ja tietoturva on jokaista koskettava haaste:

- **Julkishallintojen** on puututtava omien järjestelmiensä turvallisuuteen, ei pelkästään suojatakseen julkisen sektorin tietoja vaan myös antaakseen esimerkkiä hyvistä toimintatavoista muille toimijoille.

- **Yritysten** on käsiteltävä verkko- ja tietoturvaa ensisijaisesti voimavarana ja kilpailuedun osatekijänä eikä "negatiivisena kustannuksena".

- **Yksittäisten käyttäjien** on ymmärrettävä, että heidän kotijärjestelmänsä ovat kriittisessä asemassa kokonaisvaltaisen "turvallisuusketjun" kannalta.

Voidakseen menestyksekkäästi ratkaista edellä kuvattuja ongelmia kaikkien sidosryhmien on saatava luotettavaa tietoa tietoturvahäiriöistä ja -suuntauksista. Luotettavaa ja vertailukelpoista tietoa tällaisista häiriöistä on kuitenkin monista syistä vaikea saada. Niitä ovat muun muassa nopeus, jolla turvallisuushäiriöt voivat esiintyä, sekä joidenkin organisaatioiden haluttomuus paljastaa ja julkistaa tietoturvaloukkauksia. Turvallisuuskulttuurin luomisen peruskiviä on kuitenkin **ongelman parempi tunteminen.**

On tärkeää, että valistusohjelmat, joilla pyritään tuomaan esiin turvallisuusuhkia, eivät heikennä kuluttajien ja käyttäjien luottamusta keskittymällä pelkästään turvallisuuden kielteisiin näkökohtiin. **Verkko- ja tietoturva** onkin, aina kun se on mahdollista, **esitettävä positiivisena mahdollisuutena** pikemminkin kuin rasitteena ja kustannuksena. Sitä on tarkasteltava voimavarana, jonka avulla voidaan rakentaa kuluttajien luottamusta, tietojärjestelmiä käyttävien yritysten kilpailuetuna ja palveluntarjoajien laatukysymyksenä sekä julkisella että yksityisellä sektorilla.

Päättäjien keskeinen haaste on luoda kokonaisvaltainen lähestymistapa, jossa on yksilöitävä eri sidosryhmien tehtävät. Sen avulla on varmistettava verkko- ja tietoturvaan välittömästi tai välillisesti vaikuttavien eri julkisten politiikkojen ja säännösten asianmukainen koordinointi. Markkinoiden vapauttaminen, sääntelyn poistaminen ja lähentyminen ovat synnyttäneet eri sidosryhmiin monia eri toimijoita, mikä ei helpota tehtävää. Verkko- ja tietoturvaviraston panos on tämän tavoitteen saavuttamisessa tärkeä. Edistääkseen Euroopan tietotekniikkatoimialan kilpailukykyä ja hyvin toimivia sisämarkkinoita virasto voisi toimia keskuksena, joka jakaa tietoja, edistää yhteistyötä kaikkien sidosryhmien välillä ja vaihtaa suositeltavia käytäntöjä sekä Euroopassa että muun maailman kanssa.

3. DYNAAMINEN LÄHESTYMISTAPA TURVALLISEEN TIETOYHTEISKUNTAAN

Turvallisen tietoyhteiskunnan on perustuttava **tehokkaaseen verkko- ja tietoturvaan** ja laajalle levinneeseen **turvallisuuskulttuuriin**. Tätä varten Euroopan komissio ehdottaa **dynaamista ja yhdennettyä lähestymistapaa**, johon kaikki sidosryhmät osallistuvat ja joka perustuu **vuoropuheluun, yhteistyöhön ja vaikutusmahdollisuuksien lisäämiseen.** Koska turvallisuuskulttuurin luomisessa julkisella ja yksityisellä sektorilla on toisiaan täydentävät tehtävät, tämän alan poliittisten aloitteiden on perustuttava sidosryhmien avoimeen ja osallistavaan monenväliseen vuoropuheluun.

Tämä lähestymistapa ja siihen liittyvät toimet täydentävät ja monipuolistavat komission suunnitelmaa jatkaa kattavien ja dynaamisten toimintalinjakehysten kehittämistä useilla eri aloitteilla vuonna 2006:

(1) roskapostin ja eri uhkien, kuten vakoilu- ja muiden haittaohjelmien, kehityksen käsittely näitä erityisaiheita koskevassa tiedonannossa

(2) ehdotukset lainvalvontaviranomaisten välisen yhteistyön parantamiseksi ja sellaisten uusien rikollisuuden muotojen käsittelemiseksi, jotka hyödyntävät Internetiä ja heikentävät elintärkeiden infrastruktuurien toimintaa. Tämä on erityisen tietoverkkorikollisuutta koskevan tiedonannon aihe.

Nämä aloitteet täydentävät myös toimia, joita suunnitellaan Euroopan elintärkeiden infrastruktuurien suojaamisohjelmasta annetun komission vihreän kirjan[13] tavoitteiden saavuttamiseksi. Vihreä kirja laadittiin vastaukseksi neuvoston joulukuussa 2004 esittämään pyyntöön. Vihreällä kirjalla aloitettu prosessi johtaa luultavasti toimintasuunnitelmaan, jossa yhdistetään elintärkeiden infrastruktuurien suojelun kokonaisvaltainen lähestymistapa alakohtaisiin politiikkoihin, myös tietotekniikka-alaan. Tietotekniikkaa koskevassa alakohtaisessa politiikassa tutkittaisiin **sidosryhmien monenvälisen vuoropuhelun** avulla, mitkä ovat asiaankuuluvat taloudelliset, liike- ja yhteiskuntaelämän liikkeellepanevat voimat, jotta turvallisuutta voitaisiin tehostaa ja verkko- ja tietojärjestelmien joustavuutta lisätä.

Lisäksi sähköisen viestinnän sääntelyjärjestelmän tarkistuksessa 2006 otetaan huomioon myös verkko- ja tietoturvaa parantavat tekijät, kuten palveluntarjoajien toteuttamat tekniset ja organisatoriset toimenpiteet, tietoturvaloukkausten ilmoittamista koskevat säännökset ja velvoitteiden noudattamatta jättämisen ehkäiseminen ja seuraamukset

Ratkaisujen, palvelujen ja tietoturvatuotteiden toimittaminen loppukäyttäjille on pitkälti yksityisen sektorin asia. Siksi on strategisesti tärkeää, että **Euroopan teollisuus** on sekä tietoturvatuotteiden ja -palvelujen **vaativa käyttäjä** että verkko- ja tietoturvatuotteiden ja -palvelujen **kilpailukykyinen tarjoaja.**

Kansallisten hallitusten on kyettävä yksilöimään ja toteuttamaan parhaat toimintatavat päätöksenteossaan ja sitouduttava näkyvästi näihin tavoitteisiin hoitamalla omia tietojärjestelmiään turvallisesti. Jäsenvaltioiden ja EU:n viranomaiset ovat keskeisessä asemassa, jotta käyttäjät saavat asianmukaista tietoa, jonka avulla he voivat myötävaikuttaa omaan turvallisuuteensa. Painopisteenä on oltava tietoisuuden lisääminen verkko- ja tietoturvakysymyksistä sekä asianmukaisen ja oikea-aikaisen tiedon antaminen uhista, riskeistä ja hälytyksistä sekä parhaista toimintavoista sähköistä turvallisuutta käsittelevien Internet-portaalien kautta. Tätä tavoitetta ajatellen verkko- ja tietoturvaviraston eräs päätavoite voisi olla tutkia, onko mahdollista **perustaa monikielinen eurooppalainen tiedonjako- ja hälytysjärjestelmä**, joka perustuisi olemassa oleville tai suunnitelluille kansallisille julkisille ja yksityisille aloitteille ja linkittäisi ne yhteen.

Verkko- ja tietoturvallisuuden maailmanlaajuinen ulottuvuus vaatii komissiota lisäämään sekä kansainvälisesti että yhdessä jäsenvaltioiden kanssa ponnisteluja **edistää verkko- ja tietoturvaa koskevaa maailmanlaajuista yhteistyötä** erityisesti toteuttamalla tietoyhteiskuntahuippukokouksessa (WSIS) marraskuussa 2005 hyväksytty toimintaohjelma.

---

[13] KOM(2005) 576 lopullinen, 17.11.2005.

Lopuksi tutkimus ja kehitys auttaa erityisesti EU:n tasolla kehittämään uusia ja innovatiivisia yhteistyökumppanuuksia, joilla vauhditetaan Euroopan tietotekniikkatoimialan kasvua yleisesti ja Euroopan tietoturvatoimialan kasvua erityisesti. Komissio pyrkiikin varmistamaan, että EU:n seitsemännessä puiteohjelmassa osoitetaan riittävät rahoitusvarat verkko- ja tietoturvaa ja luotettavuustekniikoita koskevaan tutkimukseen.

3.1. Vuoropuhelu

*3.1.1. Ensimmäisenä askeleena julkisviranomaisten välisen vuoropuhelun tehostamiseksi komissio ehdottaa, että aloitetaan **kansallisten verkko- ja tietoturvaan liittyvien politiikkojen vertaileva arviointi,** mihin sisällytetään myös julkista sektoria erityisesti koskevat turvallisuuspolitiikat. Arvioinnin avulla on helpompi yksilöidä tehokkaimmat toimintatavat, jotka voidaan sitten mahdollisuuksien mukaan ottaa laajemmin käyttöön koko EU:ssa, jolloin julkishallinnoista tulee turvallisuusalan parhaiden toimintatapojen edistäjä. Sähköisellä tunnistamisella voisi esimerkiksi äskettäin hyväksytyn sähköistä hallintoa koskevan toimintasuunnitelman osana olla tässä suhteessa tärkeä asema.*

Jos arviointi organisoidaan asianmukaisesti, sen tulosten avulla voidaan myös **yksilöidä parhaat toimintatavat, joilla voidaan saada pk-yritykset ja kansalaiset tietoisiksi tarpeesta** käsitellä verkko- ja tietoturvaan liittyviä haasteita ja vaatimuksia sekä parantaa heidän valmiuksiaan tehdä niin. Verkko- ja tietoturvaviraston olisi toimittava aktiivisesti sekä tässä vuoropuhelussa että parhaiden toimintatapojen vakiinnuttamisessa ja vaihtamisessa.

*3.1.2. Tarvitaan **rakenteellista monenvälistä sidosryhmien keskustelua** siitä, miten nykyisiä välineitä ja säännöksiä voidaan parhaiten hyödyntää, jotta saadaan aikaan asianmukainen yhteiskunnallinen tasapaino turvallisuuden ja perusoikeuksien, erityisesti yksityisyyden suojelun välillä. Tähän keskusteluun tuovat oman osansa tulevalla Suomen puheenjohtajakaudella pidettäväksi suunniteltu konferenssi "*i2010 – Towards a Ubiquitous European Information Society*" (Kohti eurooppalaista ubiikkitietoyhteiskuntaa) sekä RFID:n vaikutuksia turvallisuuteen ja yksityisyyteen koskeva kuuleminen osana komission äskettäin käynnistämää laajempaa kuulemista. Lisäksi komissio järjestää*

- liikeyrityksille tarkoitetun tapahtuman, jolla pyritään saamaan teollisuus sitoutumaan turvallisuuskulttuurin tehokkaaseen toteuttamiseen **teollisuudessa**

- seminaarin, jossa pohditaan tapoja lisätä tietoisuutta turvallisuuskysymyksistä ja vahvistaa **loppukäyttäjien** luottamusta sähköisten verkkojen ja tietojärjestelmien käyttöön.

3.2. Yhteistyö

*3.2.1. Tehokkaassa päätöksenteossa on ymmärrettävä selkeästi haasteiden luonne ja laajuus. Tämä edellyttää paitsi luotettavia ja ajantasaisia tilasto- ja taloustietoja sekä tietoturvahäiriöistä että kuluttajien ja käyttäjien luottamuksen tasosta, myös ajantasaisia tietoja Euroopan tietoturvatoimialan koosta ja suuntauksista. Komissio aikoo pyytää verkko- ja tietoturvavirastoa kehittämään **luottamuksellisen kumppanuussuhteen jäsenvaltioihin ja sidosryhmiin**, jotta voidaan kehittää **asianmukainen tietojenkeruujärjestelmä,** myös menettelyt ja mekanismit*

tietoturvahäiriöitä ja kuluttajien luottamusta koskevien EU:n laajuisten tietojen keräämiseksi ja analysoimiseksi.

Koska markkinoilla on EU:ssa erityisluonne ja ne ovat voimakkaasti pirstoutuneita, komissio pyytää samanaikaisesti jäsenvaltioita, yksityistä sektoria ja tutkimusyhteisöä **luomaan strategisen kumppanuuden**, jotta voidaan varmistaa, että käytettävissä on tietoja tietoturvatoimialasta ja tuotteiden ja palvelujen kehittyvistä markkinasuuntauksista EU:ssa.

3.2.2. Jotta Euroopan valmiuksia vastata verkkoturvauhkiin voitaisiin parantaa, komissio pyytää verkko- ja tietoturvavirastoa tutkimaan, ***onko mahdollista toteuttaa eurooppalainen tiedonjako- ja hälytysjärjestelmä****, jolla voidaan edistää tehokkaita tapoja reagoida nykyisiin ja tuleviin sähköisten verkkojen uhkiin. Tällaisen järjestelmän edellytys on monikielinen EU-portaali, joka antaa kohdennettua tietoa uhista, riskeistä ja hälytyksistä.*

3.3. Vaikutusmahdollisuuksien lisääminen

Kunkin sidosryhmän vaikutusvallan lisääminen on edellytys tietoisuuden lisäämiseksi tietoturvatarpeista ja -riskeistä, jotta verkko- ja tietoturvaa voidaan parantaa.

3.3.1. Tähän liittyen komissio pyytää ***jäsenvaltioita***

- osallistumaan aloitteellisesti ehdotettuun kansallisten verkko- ja tietoturvapolitiikkojen vertailevaan arviointiin
- edistämään läheisessä yhteistyössä verkko- ja tietoturvaviraston kanssa tiedotuskampanjoita tehokkaiden tietoturvatekniikoiden, -käytäntöjen ja -menetelmien eduista, hyödyistä ja tuloksista
- käynnistämään sähköisiä hallintopalveluja ja edistämään hyviä tietoturvakäytäntöjä, jotka voitaisiin sitten ulottaa myös muille aloille
- kannustamaan verkko- ja tietoturvaohjelmien kehittämistä osana korkea-asteen koulutuksen opetussuunnitelmaa.

3.3.2. *Komissio pyytää myös* ***yksityisen sektorin*** *sidosryhmiä tekemään aloitteita, jotta voitaisiin*

- kehittää asianmukainen määritelmä ohjelmistotuottajien ja Internet-palveluntarjoajien vastuusta suhteessa riittävän ja todennettavan tietoturvatason tarjoamiseen. Tähän tarvitaan sellaisten vakioitujen prosessien tukea, jotka täyttävät yleisesti hyväksytyt turvastandardit ja parhaita toimintatapoja koskevat säännöt.
- edistää monimuotoisuutta, avoimuutta, yhteentoimivuutta, käytettävyyttä ja kilpailua tietoturvan avaintekijöinä sekä lisätä tietoturvaa tehostavien tuotteiden, prosessien ja palvelujen käyttöönottoa käyttäjätunnusvarkauksien ja muiden yksityisyyttä loukkaavien hyökkäysten ehkäisemiseksi ja torjumiseksi

- levittää hyviä tietoturvatoimintoja verkko-operaattoreille, palveluntarjoajille ja pk-yrityksille tietoturvan ja liiketoiminnan jatkuvuuden perusedellytyksinä

- edistää liikealan, erityisesti pk-yritysten, koulutusohjelmia, jotta työntekijöillä on tarvittavat tiedot ja taidot tehokkaiden tietoturvakäytäntöjen toteuttamiseen.

- pyrkiä luomaan kohtuuhintaiset turvavarmentamisjärjestelmät sellaisille tuotteille, prosesseille ja palveluille, jotka koskevat EU:n erityisiä tarpeita (erityisesti yksityisyyteen liittyen)

- ottaa vakuutusala mukaan kehittämään asianmukaiset riskinhallintavälineet ja -menetelmät tietoteknisten riskien käsittelemiseksi ja edistää riskinhallintakulttuuria eri organisaatioissa ja yrityksissä (erityisesti pk-yrityksissä).

4. PÄÄTELMÄT

EU:n tietojärjestelmiin ja -verkkoihin liittyvien turvallisuushaasteiden tunnistaminen ja kohtaaminen edellyttää kaikkien sidosryhmien täysimääräistä sitoutumista. Tämä pyritään saavuttamaan tässä tiedonannossa hahmotellulla lähestymistavalla: vahvistamalla **sidosryhmien monenvälistä lähestymistapaa.** Se perustuisi yhteisiin etuihin, kunkin osapuolen tehtävien yksilöimiseen ja dynaamisten puitteiden luomiseen tehokkaan julkisen päätöksenteon ja yksityisen sektorin aloitteiden edistämiseksi.

Komissio raportoi vuoden 2007 puolivälissä neuvostolle ja parlamentille aloitetuista toiminnoista, alustavista havainnoista ja yksittäisten aloitteiden etenemisestä, myös verkko- ja tietoturvaviraston, jäsenvaltioiden ja yksityisen sektorin tekemien aloitteiden osalta. Tarvittaessa komissio ehdottaa verkko- ja tietoturvallisuuden suositusta.

EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 31.5.2006
KOM(2006) 251 slutlig

MEDDELANDE FRÅN KOMMISSIONEN TILL RÅDET, EUROPAPARLAMENTET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN

En strategi för ett säkert informationssamhälle – ”Dialog, partnerskap och användarinflytande”

{SEK(2006) 656}

INNEHÅLL

MEDDELANDE FRÅN KOMMISSIONEN TILL RÅDET, EUROPAPARLAMENTET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN

En strategi för ett säkert informationssamhälle – ”Dialog, partnerskap och användarinflytande”

1. INLEDNING

Meddelandet ”i2010 – Det europeiska informationssamhället för tillväxt och sysselsättning”[1] visade hur viktigt det är med nätverks- och informationssäkerhet om man vill skapa ett gemensamt informationsområde i EU. Vår ekonomi och vårt samhälles alla strukturer blir allt mer beroende av nätverkens och informationssystemens tillgänglighet, tillförlitlighet och säkerhet.

Syftet med detta meddelande är att blåsa nytt liv i Europeiska kommissionens strategi så som den beskrivs i 2001 års meddelande *Nät och informationssäkerhet: förslag till en europeisk strategi*[2]. Där redogörs det för de säkerhetshot som informationssamhället utsätts för i dag, och för vad som kan göras för att öka nätverks- och informationssäkerheten.

Målet är att utgående från de erfarenheter som medlemsstaterna och Europeiska gemenskapen gjort vidareutveckla en dynamisk och omfattande strategi för EU, grundad på en säkerhetskultur och på **dialog, partnerskap och användarinflytande.**

Europeiska gemenskapen har utvecklat ett tredelat system för att bekämpa informationssamhällets säkerhetsproblem, nämligen med specifika åtgärder för nätverks- och informationssäkerhet, de rättsliga ramarna för elektronisk kommunikation (som också omfattar integritetsskydd och skydd av personuppgifter), samt kompen mot databrottsligheten. Dessa tre aspekter kan visserligen i viss mån behandlas var och en för sig, men de hänger ihop på många punkter, vilket nödvändiggör en samordnad strategi. I detta meddelade beskrivs strategin och ramarna för vidareutvecklad och förbättrad hantering av nätverks- och informationssäkerheten.

I 2001 års meddelande beskrivs nätverks- och informationssäkerheten som ”*förmågan hos ett nät att tåla, vid en viss tillförlitlighetsnivå, olyckshändelser eller illvilligt uppträdande som äventyrar tillgängligheten, äktheten (autentisering), integriteten och konfidentialiteten hos lagrade eller vidarebefordrade data och besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät*.” På senare år har Europeiska gemenskapen gjort en rad insatser för att förbättra nätverks- och informationssäkerheten.

De rättsliga ramarna för elektronisk kommunikation håller på att ses över. De omfattar även säkerhetsbestämmelser. Bland annat innehåller direktivet om integritet och elektronisk kommunikation[3] en bestämmelse om att de som tillhandahåller offentligt tillgängliga tjänster

---

1 KOM(2005) 229 slutlig av den 1 juni 2005.
2 KOM(2001) 298 slutlig av den 6 juni 2001.
3 Direktiv 2002/58/EG.

för elektronisk kommunikation måste garantera tjänsternas säkerhet. Dessutom fastställs bestämmelser om skräppost[4] och spionprogram[5].

Förtroende och säkerhet är också viktiga frågor i Europeiska gemenskapens program för forskning och utveckling. I sjätte ramprogrammet för forskning tas dessa frågor upp i en mängd olika projekt. Säkerhetsrelaterad forskning skall förstärkas ytterligare i sjunde ramprogrammet, genom att det inrättas ett europeiskt program för säkerhetsforskning[6]. Programmet *Safer Internet Plus* ger dessutom stöd till nätverksprojekt och till utbyte av effektiva metoder för att bekämpa skadliga innehåll som cirkulerar inom informationsnäten.

Som en del av insatserna mot säkerhetshoten beslöt Europeiska kommissionen år 2004 att skapa Europeiska byrån för nät- och informationssäkerhet (ENISA). Byrån bidrar till utvecklingen av en säkerhetskultur för nätverk och information som gagnar allmänheten, konsumenterna, företagen och den offentliga sektorns organisationer över hela EU.

EU spelar också en aktiv roll i de olika internationella fora som behandlar dessa frågor, till exempel OECD, Europarådet och FN. Vid världstoppmötet om informationssamhället i Tunis gav EU ett kraftigt bidrag till diskussionen om tillgänglighet, tillförlitlighet och säkerhet för nätverk och information. Tunisagendan[7], som tillsammans med Tunisåtagandet fastställer nästa etapper i den strategiska debatten om det globala informationssamhället så som det förespråkas av världens ledare, pekar på behovet av fortsatt kamp mot databrottslighet och skräppost samtidigt som privatlivet och yttrandefriheten skyddas. TAIS slår även fast att det för att få en gemensam förståelse för frågorna om Internetsäkerhet behövs ytterligare samarbete för att underlätta insamling och spridning av säkerhetsrelaterad information och utbyte av god praxis bland alla berörda parter i fråga om hur man kan bekämpa säkerhetsriskerna.

2. ETT SÄKRARE INFORMATIONSSAMHÄLLE: DE VIKTIGASTE FRÅGORNA

Trots ansträngningar på internationell, europeisk och nationell nivå är säkerheten fortfarande ett mycket trängande problem.

Bakom anfallen mot informationssystemen ligger allt oftare vinstlystnad, och inte bara en önskan att skapa störningar för sakens egen skull. Uppgifter samlas olagligen och allt oftare utan att användarna ens vet om det, och de olika typerna av sabotageprogram[8] (och deras utvecklingstakt) ökar snabbt. Ett bra exempel på denna utveckling är skräpposten: den har blivit en inkörsport för virus, bedrägerier och annan brottslig verksamhet, som spionprogram, phishing[9] och andra former av sabotageprogram. Skräpposten sprids i allt större utsträckning

---

4 Oönskade kommersiella meddelanden.

5 Spionprogram är mjukvara som sätts in utan adekvat förvarning och utan användarens medgivande eller kontroll.

6 Detta förbereds för närvarande genom en förberedande åtgärd för säkerhetsforskning som pågår under från 2004 till slutet av 2006.

7 För ett globalt partnerskap i informationssamhället: Uppföljning av Tunisfasen av världstoppmötet om informationssamhället (WSIS), KOM(2006)181 slutlig av den 27 april 2006.

8 Sabotageprogram, på engelska malware.

9 Phishing är en form av Internetbedrägeri där värdefulla uppgifter som kreditkortsnummer, bankkontonummer, användarnamn och lösenord stjäls.

genom botnets[10], dvs. servrar och datorer som har tagits över och används utan ägarnas vetskap.

Allt eftersom mobila apparater (inbegripet tredje generationens mobiltelefoner, bärbara datorspel osv.) och mobilbaserade nättjänster blir vanligare uppstår nya problem, när IP-baserade tjänster utvecklas i snabb takt. De kan så småningom bli en vanligare väg för attacker än persondatorerna, eftersom persondatorerna redan har utvecklat en betydande säkerhetsnivå. Alla nya former av kommunikationsplattformar och informationssystem ger oundvikligen nya inkörsportar för illvilliga attacker.

En annan betydelsefull utveckling är uppkomsten av intelligenta miljöer där intelligenta apparater med stöd av dator- och nätverksteknik finns överallt (t.ex. genom RFID[11], IPv6 och sensornät). En fullständigt sammankopplad och länkad vardag kan ge enorma möjligheter. Men den medför också nya säkerhets- och integritetsrelaterade risker. Gemensamma plattformar och tillämpningar innebär visserligen en stor förbättring av driftskompatibiliteten och spridningen av informations- och kommunikationstekniken (IKT) men de kan även medföra risker. Ju mer standardmjukvara som används, till exempel, desto större blir följderna när någon utnyttjar mjukvarans svagheter eller den uppvisar fel. Uppkomsten av ”monokulturer” av mjukvaruplattformar och tillämpningar kan underlätta tillväxten och spridningen av säkerhetsrisker som sabotageprogram och virus enormt. **Diversitet, öppenhet och driftskompatibilitet är viktiga säkerhetsaspekter och bör främjas**.

IKT-sektorns betydelse för Europas ekonomi och samhälle är obestridlig. Den är av avgörande betydelse för nyskapande och bidrar med nästan 40 % av produktivitetstillväxten. Dessutom är den i sig själv en ytterst innovativ sektor som står för över en fjärdedel av EU:s sammanlagda FoU-insatser. Den bidrar också kraftigt till ekonomisk tillväxt och sysselsättning i näringslivets alla sektorer. Allt fler européer lever i ett verkligt informationsbaserat samhälle där IKT-användningen ökar explosionsartat och har blivit en grundläggande funktion i människornas sociala och ekonomiska samspel. Enligt Eurostat använde 89 % av EU:s företag Internet aktivt år 2004 och ungefär 50 % av konsumenterna hade nyligen använt Internet[12].

Luckor i nät- och informationssäkerheten kan få effekter som vida överskrider den ekonomiska dimensionen. Man oroar sig allmänt för att säkerhetsproblem kan avskräcka användare och minska spridningen av IKT, vars tillgänglighet, tillförlitlighet och säkerhet är förutsättningar för att människors grundläggande rättigheter skall kunna garanteras på nätet.

Med den ökande sammanlänkningen mellan nät blir dessutom andra viktiga infrastrukturer som exempelvis transport och energi allt mer beroende av att deras informationssystem är säkra.

riskerna underskattas fortfarande både av EU:s företag och av allmänheten. Detta har många orsaker, men den viktigaste orsaken för företag tycks vara att avkastningen av investeringar i säkerhet syns så dåligt. För allmänheten är det främst det faktum att de inte känner till sitt ansvar i fen globala säkerhetskedjan som är avgörande.

---

10 Botnets är nätsamanslutningar av s.k. ”bots”, dvs. tillämpningar som genom fjärrstyrning utför uppgifter åt någon annan, och som i hemlighet installerats på offrets dator.

11 Radiofrekvensidentifiering.

12 Eurostat, Internet activities in the European Union, 40/2005.

Eftersom IKT och informationssystem finns överallt är nät- och informationssäkerhet en fråga som berör alla.

- **Offentliga myndigheter** måste se till att deras system är säkra, och inte bara för att skydda information inom den offentliga sektorn, utan också för att föregå med gott exempel och visa andra aktörer bästa praxis.

- **Företag** måste se nät- och informationssäkerhet mer som en tillgång och en del av deras konkurrensövertag än som en ”negativ utgift”.

- De **enskilda användarna** måste förstå att deras hemsystem är en viktig länk i den allmänna ”säkerhetskedjan”.

För att på bästa sätt lösa de problem som nämnts behöver de berörda parterna tillförlitliga uppgifter om händelser och utvecklingar som berör informationssäkerheten. Det är emellertid av många orsaker svårt att komma åt tillförlitliga och kompletta uppgifter om sådana händelser. Bland annat sker säkerhetstillbuden ofta mycket hastigt, och många organisationer är också mycket ovilliga att erkänna och offentliggöra brott mot deras säkerhet. En grundförutsättning om man vill utveckla en säkerhetskultur är emellertid att vi **ökar vår kunskap om problemen.**

Det är viktigt att informationskampanjer avsedda att belysa säkerhetsrisker inte undergräver konsumenternas och användarnas förtroende och tillit genom att enbart lyfta fram de negativa säkerhetsaspekterna. Man bör därför överallt där så är möjligt **presentera nät- och informationssäkerhet som en dygd och en möjlighet** snarare än ett riskmoment och en kostnadsfaktor. Det är viktigt att säkerheten ses som en tillgång för att bygga upp förtroende och vinna konsumenternas tillit, en konkurrensfördel för företag som driver informationssystem och en fråga om tjänstekvalitet för tjänsteleverantörer både inom den offentliga och den privata sektorn.

Det viktigaste målet för beslutsfattarna är att få till ett holistiskt tillvägagångssätt. Därvid måste man se de olika berörda parternas respektive roll i sammanhanget. Samordning mellan de olika offentliga strategier och rättsliga bestämmelser som direkt eller indirekt påverkar nät- och informationssäkerheten måste garanteras. Liberaliseringen, avregleringen och sammanflätningen har lett till de olika grupperna av berörda parter består av en mångfald olika aktörer, vilket inte gör saken lättare. ENISA kan bidra kraftigt till att detta mål uppnås. Byrån kan fungera som ett forum för utbyte av information, samarbete mellan alla parter och information om bästa metoder, både inom EU och med den övriga världen. På så sätt kan byrån bidra till IKT-sektorns konkurrenskraft och till en väl fungerande inre marknad.

3. EN DYNAMISK STRATEGIS FÖR ETT SÄKERT INFORMATIONSSAMHÄLLE

Ett säkert informationssamhälle måste utgå från **ökad nät- och informationssäkerhet** och en väletablerad **säkerhetskultur**. Därför föreslår Europeiska kommissionen en **dynamisk och samordnad strategi** som omfattar alla berörda parter och grundas på **dialog och användarinflytande**. Den offentliga och den privata sektorn kompletterar varandra i skapandet av en säkerhetskultur, och därför måste strategiska initiativ på detta område utgå från en **öppen dialog mellan alla berörda parter**.

Under loppet av 2006 kommer denna strategi och tillhörande insatser att komplettera och berika den vidare utvecklingen av kommissionens plan för en omfattande och dynamisk strategisk ram.

(1) Utvecklingen av skräppost och andra hot, som spionprogram och andra former av sabotageprogram skall tas upp i ett meddelande om dessa frågor.

(2) Förslag om förbättrat samarbete mellan regleringsmyndigheter, och om hanteringen av nya former av brottslighet som utnyttjar Internet och undergräver viktiga infrastrukturer skall läggas fram. Detta kommer att tas upp i ett särskilt meddelande om databrottslighet.

Dessa initiativ kompletterar dessutom de insatser som planeras för att uppnå målen i kommissionens grönbok om ett europeiskt program för skydd av kritisk infrastruktur[13], som utarbetats på begäran av rådet i december 2004. Grönboken väntas leda till en handlingsplan som kombinerar en allmän, övergripande strategi för skydd av kritisk infrastruktur med de nödvändiga sektorsspecifika strategierna, bland annat en för IKT-sektorn. Den sektorsbundna strategin för IKT-sektorn skulle, genom en **dialog mellan de berörda parterna**, undersöka de viktigaste ekonomiska, företagsmässiga och samhälleliga drivkrafterna i syfte att öka nätverkens och informationssystemens säkerhet och motståndskraft.

Dessutom kommer man i 2006 års genomgång av regelverket för elektronisk kommunikation att undersöka hur nät- och informationssäkerheten kan förbättras, till exempel genom tjänsteleverantörernas tekniska och organisatoriska insatser, bestämmelser om hur man handskas med säkerhetsbrott och specifika lösningar på och påföljder för dem som inte uppfyller sina skyldigheter.

Det är i första hand den privata sektorn som skall förse slutanvändarna med lösningar, tjänster och säkerhetsprodukter. Därför är det strategiskt viktigt att **den europeiska industrin både är en krävande användare** av säkerhetsprodukter och –tjänster, och **en konkurrenskraftig leverantör** av nät- och informationssäkerhetsprodukter och –tjänster.

Nationella regeringar måste kunna identifiera och införa de bästa metoderna i sin politik, och samtidigt visa sitt engagemang för dessa politiska mål genom att sköta sina egna informationssystem på ett säkert sätt. Offentliga myndigheter, både i medlemsstaterna och på EU-nivå, har en viktig uppgift i att informera användarna korrekt så att dessa kan bidra till sin egen säkerhet. En prioritering bör vara att öka medvetenheten om nät- och informationssäkerhet och ge korrekt information i rätt ögonblick genom särskilda e-säkerhetsservrar, både om hot, risker och varningar, och om bästa metoder. Ett viktigt mål för Europeiska byrån för nät- och informationssäkerhet (ENISA) skulle därför kunna vara att undersöka möjligheterna att **skapa ett EU-omfattande, flerspråkigt system för informationsutbyte och alarmering** som kunde utgå ifrån och länka samman befintliga och planerade nationella initiativ, både på den offentliga och den privata sektorn.

Nät- och informationssäkerhetens globala dimension innebär att kommissionen både internationellt och i samordning med medlemsstaterna måste öka sina ansträngningar att **främja ett globalt samarbete om nät- och informationssäkerhet**, bland annat genom att

[13] KOM(2005) 576 slutlig, 17.11.2005.

genomföra den dagordning som antogs vid världstoppmötet om informationssamhället i november 2005.

Slutligen kan forskning och utveckling, inte minst på EU-nivå, bidra till uppkomsten av nya och nyskapande samarbeten som kan driva på den europeiska IKT-industrins tillväxt, och då särskilt främja den europeiska IKT-säkerhetsindustrin. Kommissionen kommer därför att försöka se till att det inom EU:s sjunde ramprogram avsätts tillräckliga ekonomiska resurser för forskning om när- och informationssäkerhet och tillförlitlig teknik.

3.1. Dialoger

3.1.1. Som ett första steg för att förbättra dialogen mellan offentliga myndigheter föreslår kommissionen att inleda en ***jämförelse mellan medlemsstaternas nät- och informationssäkerhetsrelaterade strategier,*** *inbegripet särskilda säkerhetsstrategier för den offentliga sektorn. Denna riktmärkning kan bidra till att ta fram bästa metoder som sedan kan tillämpas mer allmänt i EU och göra de offentliga förvaltningarna till drivfjädrar i fråga om goda säkerhetsmetoder. De insatser som görs i fråga om elektronisk identifiering, till exempel inom ramen för den nya handlingsplanen för e-förvaltning, kan spela en viktig roll i detta sammanhang.*

Resultaten från en sådan jämförelse skulle, om de struktureras på rätt sätt, göra det möjligt att **hitta de bästa metoderna för att bland de små och medelstora företagen och allmänheten öka medvetenheten om att de själva måste** ta itu med sina specifika nät- och informationssäkerhetsfrågor och –krav, och se om de är i stånd att göra detta. ENISA skulle kunna spela en aktiv roll i denna dialog och bidra till konsolidering och utbyte av bästa metoder.

3.1.2. Den behövs en ***strukturerad debatt mellan alla berörda parter*** *om hur man bäst kan utnyttja befintliga instrument och rättsakter för att uppnå den balans som samhället behöver mellan säkerhet och skydd av grundläggande rättigheter som privatlivet. Den planerade konferensen ”i2010 – Towards a Ubiquitous European Information Society” (i2010 – Mot ett europeiskt informationssamhälle för alla), som skall organiseras av det påföljande finska ordförandeskapet, och samrådet om radiofrekvensidentifieringens konsekvenser för säkerhet och skydd av privatlivet, som ingår i det mer allmänna samråd som kommissionen nyligen inlett, kommer att bidra till denna debatt. Kommissionen kommer bland annat också att organisera följande:*

- Ett företagsevenemang för att främja näringslivets engagemang för att finna effektiva sätt att införa en säkerhetskultur **inom näringslivet.**

- Ett seminarium om hur man kan öka medvetenheten om säkerhetsfrågor och förstärka **slutanvändarnas** förtroende för nya elektroniska nät och informationssystem.

3.2. Partnerskap

3.2.1. Det är viktigt att verkligen förstå problemens art och omfattning om man skall kunna föra en effektiv politik. Därför behövs det inte bara tillförlitliga och aktuella statistiska och ekonomiska uppgifter om informationssäkerhetstillbud och konsumenternas och användarnas grad av förtroende, utan också aktuella uppgifter

om hur stor IKT-säkerhetsindustrin i EU är och åt vilket håll den utvecklas. Kommissionen har för avsikt att be ENISA att utveckla ***ett förtroendefullt samarbete med medlemsstaterna och de berörda parterna*** *för att utarbeta* ***ramar för datainsamling****, dvs. förfaranden och mekanismer för att samla in och analysera EU-omfattande uppgifter om säkerhetstillbud och konsumenternas förtroende.*

Eftersom EU:s marknader är så uppsplittrade och ofta specifika till sin natur kommer kommissionen samtidig att uppmana medlemsstaterna, den privata sektorn och forskningssamfundet att **utveckla ett strategiskt samarbete** för att garantera tillgången till uppgifter om IKT-säkerhetsindustrin och marknadstendenserna för produkter och tjänster i EU.

3.2.2. I syfte att förbättra EU:s möjligheter att bemöta nätsäkerhetshot kommer kommissionen att be ENISA att undersöka ***om det är möjligt att skapa ett europeiskt system för informationsutbyte och varning*** *som kan underlätta effektiva reaktioner på befintliga och nytillkomna hot mot elektroniska nät. En förutsättning för ett sådant system vore en* ***flerspråkig EU-portal*** *som kan e skräddarsydd information om hot, risker och varningar.*

3.3. Delaktighet

De olika berörda parternas delaktighet är en förutsättning för att man skall kunna öka medvetenheten om säkerhetsbehov och –risker och främja nät- och informationssäkerheten.

3.3.1. Därför vill kommissionen uppmana ***medlemsstaterna*** *att*

- på ett föregripande sätt delta i den föreslagna jämförelsen av nationella strategier för nät- och informationssäkerhet,
- i nära samarbete med ENISA främja informationskampanjer om fördelarna och vinsterna med att införa effektiv säkerhetsteknik och effektiva metoder och beteenden,
- driva på spridningen av e-förvaltningstjänster för att informera om och främja goda säkerhetsmetoder som sedan kan spridas till andra sektorer,
- främja utvecklingen av program för nät- och informationssäkerhet som del av högskolornas läroplaner.

3.3.2. *Kommissionen uppmanar också de berörda parterna inom den* ***privata sektorn*** *att ta initiativ för att*

- utveckla en lämplig definition av det ansvar som vilar på tillverkarna av mjukvara och Internets tjänsteleverantörer i fråga om att tillhandahålla lämpliga och kontrollerbara säkerhetsnivåer, (här krävs stöd till standardiserade förfaranden som kan uppfylla gemensamt överenskomna säkerhetsnormer och bestämmelser om bästa praxis),
- främja diversifiering, öppenhet, driftskompatibilitet, användarvänlighet och konkurrenskraft som drivfjädrar för säkerhet, och uppmuntra till användning av

säkerhetshöjande produkter, förfaranden och tjänster som kan motverka och bekämpa id-stöld och andra angrepp på privatlivets skydd,

- sprida god säkerhetsmetodik för nätoperatörer, tjänsteleverantörer och små- och medelstora företag som en slags grundnivå för säkerhet och kontinuitet i fråga om verksamheten,

- främja utbildningsprogram inom affärssektorn, inte minst för små och medelstora företag, så att de anställda får den kunskap och de färdigheter som behövs för att effektivt tillämpa säkerhetsmetoderna,

- sträva efter betalbara system för säkerhetscertifiering för produkter, processer och tjänster som kan uppfylla EU:s särskilda behov (inte minst i fråga om skydd av privatlivet),

- engagera försäkringssektorn i utvecklingen av lämpliga riskhanteringsverktyg och metoder för att hantera IKT-relaterade risker och främja en riskhanteringskultur inom organisationer och företag (inte minst små och medelstora företag).

4. SLUTSATSER

Alla berörda parter måste vara aktivt delaktiga om man skall kunna identifiera och lösa säkerhetsproblemen kring informationssystem och nätverk i EU. Den strategi som skildras i detta meddelande vill uppnå detta genom att uppmuntra till **insatser där flera berörda parter samarbetar**. Detta skulle bygga på gemensamt intresse, och de olika parternas respektive roll skulle framhävas. Därigenom skulle man utveckla en dynamisk ram för att främja en effektiv offentlig beslutsprocess och effektiva insatser från den privata sektorn.

I mitten av 2007 kommer kommissionen att rapportera till rådet och Europaparlamentet om vilka insatser som inletts och vad man hittills kommit fram till, samt hur långt man kommit med de olika insatserna (inbegripet ENISA:s verksamhet och medlemsstaternas och den privata sektorns insatser). Vid behov kommer kommissionen att föreslå en rekommendation om nät- och informationssäkerhet.